Instituto Politécnico Formosa

NACE WIKILEAKS(2006)

Integrantes

- Aquino Nazarena
- Leger Axel
- Pzocik Brandon
- Franco Mirna
- Ocampo Emiliano

Institución

Instituto Politécnico Formosa

Carrera

Tec. Sup. Desarrollo de Software Multiplataforma

Materia

Seminario Actualización III: Ciberseguridad

Profesores

- Alejandro Sanabria
- Alejandro Ruiz Diaz

Fecha

Agosto 28, 2025

ÍNDICE

Introducción

- Breve presentación del tema

Un leaking es hacer pública alguna información confidencial o secreta sin contar con autorización o aprobación oficial, estas filtraciones pueden ser intencionales o accidentales. y para los gobiernos u organizaciones afectadas pueden tener efectos en la percepción de la opinión pública y efectos en la diplomacia.

Si la información filtrada es confidencial o clasificada (como informes financieros, datos personales o secretos de Estado), puede constituir el delito de violación de secretos.

En Argentina, por ejemplo, el artículo 156 del Código Penal castiga a quien revele secretos obtenidos por su oficio o cargo.

WikiLeaks es una página web que publica documentos e imágenes generalmente filtrados por fuentes no identificadas públicamente con el fin de revelar escándalos y casos de corrupción que consideran de interés público. Creada por Julian Assange y un grupo de programadores, periodistas y activistas.

Permitiendo a la comunidad global analizar, discutir y contextualizar los documentos publicados, la organización se convirtió en un fenómeno global al difundir información sensible que expuso casos de corrupción, abusos militares y prácticas secretas de gobiernos y corporaciones.

Según su propia web *“Wikileaks desarrolla una versión no censurable de Wikipedia para la publicación masiva y el análisis de documentos secretos ("Leaks"), manteniendo a sus autores en el anonimato”*.

Su nombre viene de "Wiki" proviene del término hawaiano "rápido" y “Leaks” del inglés filtraciones.

- Motivaciones que llevaron a crear el sitio

A principios de los 2000, se consolidó una comunidad global de hackers y activistas digitales que promueven la transparencia, la libertad de información y la resistencia al control estatal.

Tras los atentados del 11-S en 2001, Estados Unidos y otros países intensificaron la vigilancia, el secretismo y las operaciones militares encubiertas, lo que llevó a crear una plataforma para publicar filtraciones de forma segura y anónima.

- Nacimiento y primeras publicaciones

Julian Assange nació el 3 de julio de 1971 en Queensland, Australia.

De adolescente y a los 20 años, Assange se convirtió en un hábil y prolífico hacker, conocido en la comunidad australiana de piratas informáticos como Mendax. En 1996,

Assange se declaró culpable de 24 delitos de piratería informática ante el Tribunal del Condado de Victoria, en Melbourne.

Aunque el juez calificó los presuntos delitos de “bastante graves”, también dijo que Assange estaba motivado por “curiosidad intelectual” y no por malicia. Finalmente, Assange fue multado y puesto en libertad (Klimentov, M. 25 de junio de 2014).

Assange, partidario de la libre circulación de información, registró en 1999 el nombre de dominio Wikileaks.org, pero no lo empezó a usar activamente hasta 2006. Ese año transformó febrilmente el sitio web en un lugar seguro para los denunciantes, específicamente para aquellos que quisieran brindar documentos secretos para su difusión pública .

WikiLeaks recibió su primer lote de documentos sensibles no de un denunciante sino de The Onion Router (Tor), una red de cifrado diseñada para permitir a los usuarios transmitir datos de forma anónima. Un voluntario de WikiLeaks extrajo los datos provenientes de Tor, recopilando más de un millón de documentos y proporcionando al sitio su primera primicia: un mensaje de un líder rebelde somalí que incitaba al uso de sicarios para asesinar a funcionarios del gobierno. Se publicó en el sitio en diciembre de 2006. La autenticidad del documento nunca se verificó.(Ray M, 2025)

Las filtraciones más importantes de Wikileaks

- 2010 – Video “Collateral Murder”

5 de abril de 2010 WikiLeaks ha publicado un vídeo militar clasificado de EE.UU. que muestra el asesinato indiscriminado de más de una docena de personas en el suburbio iraquí de Nueva Bagdad, incluidos dos empleados de noticias de Reuters.

Reuters ha intentado obtener el video a través de la Ley de Libertad de Información, sin éxito desde el momento del ataque. El video, grabado desde la mira de un helicóptero Apache, muestra claramente el asesinato no provocado de un empleado de Reuters herido y sus rescatadores. Dos niños pequeños que participaron en el rescate también resultaron gravemente heridos.

Los militares no revelaron cómo murió el personal de Reuters y declararon que no sabían cómo resultaron heridos los niños.

Tras las peticiones de la agencia Reuters, se investigó el incidente y el ejército estadounidense concluyó que las acciones de los soldados se ajustaron al derecho de los conflictos armados y a sus propias "Reglas de enfrentamiento".

En consecuencia, WikiLeaks ha publicado las Reglas de Compromiso clasificadas para 2006, 2007 y 2008, revelando dichas reglas antes, durante y después de los asesinatos.

WikiLeaks ha publicado tanto el vídeo original de 38 minutos como una versión más corta con un análisis inicial. Ambas versiones tienen subtítulos de las transmisiones de radio.

WikiLeaks obtuvo este video, así como documentos de apoyo, de varios denunciantes militares. WikiLeaks se esfuerza al máximo para verificar la autenticidad de la información que recibe. Hemos analizado la información sobre este incidente a partir de diversas fuentes. Hemos hablado con testigos y periodistas directamente involucrados en el incidente.

WikiLeaks quiere asegurarse de que toda la información filtrada que recibe reciba la atención que merece. En este caso particular, algunas de las personas asesinadas eran periodistas que simplemente hacían su trabajo: arriesgaban sus vidas para informar sobre la guerra. Irak es un lugar muy peligroso para los periodistas: entre 2003 y 2009, 139 periodistas fueron asesinados en el ejercicio de su profesión.

- 2010 – War Logs (registros de Guerra de Afganistán e Irak)

El 22 de octubre del 2010, WikiLeaks publicó mas de 391.000 **documentos clasificados** sobre las guerras de Afganistán y de Irak, conocidos como los *Afghanistan War Logs* y los *Iraq War Logs*. Estas filtraciones constituyen las **mayores en la historia del ejército estadounidense**, y provienen de **informes de campo de soldados**, extraídos de una base de datos del Pentágono que registran día a día incidentes, operaciones, ataques, arrestos y movimientos de tropas. Los documentos ofrecen un **diario detallado de ambos conflictos**, mostrando la guerra tal como la vivían los soldados sobre el terreno.

Los registros revelan cómo, a pesar de la superioridad militar de Estados Unidos, las fuerzas se enfrentaron a **guerras asimétricas** en las que insurgentes y grupos locales podrían causar daños significativos y poner en riesgo tanto a soldados como a civiles. Los documentos incluyen información sobre **muertes, secuestros, torturas, ataques y violencia cotidiana**, así como la participación de países vecinos en los conflictos.

En el caso de Irak, se incluye el famoso incidente del **12 de julio de 2007**, conocido como *Collateral Murder*, donde helicópteros estadounidenses dispararon contra civiles, incluyendo periodistas de Reuters y niños, mostrando los errores y horrores de la guerra.

Los informes documentan más de **109.000 muertes en Irak** entre 2004 y 2009, entre ellas:

- 3.884 soldados estadounidenses
- 224 soldados aliados
- Más de 8.000 miembros de las fuerzas de seguridad iraquíes
- Más de 92.000 civiles

En Afganistán, los Afghanistan War Logs revelan cerca de **77.000 informes de campo**, mostrando también operaciones, ataques, bajas y la dificultad de las tropas estadounidenses para controlar el territorio, así como el impacto sobre la población civil.

Ambas filtraciones evidencian la brecha entre la narrativa oficial y la realidad del conflicto, mostrando que las guerras fueron más largas y costosas de lo declarado. Además, permiten reconstruir los efectos sociales y humanos de los conflictos, incluyendo la violencia sectaria, el miedo constante y las dificultades cotidianas que enfrentan soldados y civiles.

- 2010 – Cables diplomáticos

El 28 de noviembre de 2010, WikiLeaks dio a conocer lo que se conoció como Cablegate, una de las mayores filtraciones de la historia. Se trató de más de 250.000 documentos secretos del Departamento de Estado de Estados Unidos, que abarcaban desde 1966 hasta febrero de 2010. Estos cables diplomáticos fueron obtenidos por la entonces soldado Chelsea Manning y exponían comunicaciones confidenciales entre más de 270 embajadas estadounidenses y Washington.

La publicación tuvo un impacto mundial: generó crisis diplomáticas en distintos países, obligó a embajadores a renunciar y despertó indignación en numerosos gobiernos. La administración de Barack Obama condenó duramente la filtración y consideró a Julian Assange, fundador de WikiLeaks, como una amenaza para la seguridad nacional. Incluso, según investigaciones posteriores, funcionarios de la CIA llegaron a debatir la posibilidad de asesinarlo.

Los documentos revelaban aspectos inéditos de la política exterior de Estados Unidos. Entre las filtraciones más relevantes se encontraban los ataques encubiertos con misiles en Yemen, las preocupaciones sobre el arsenal nuclear de Pakistán, los pedidos del rey saudí Abdullah para que Washington atacara a Irán, así como descripciones muy poco diplomáticas de líderes mundiales, por ejemplo, caracterizando a Vladimir Putin como un “macho alfa” o comparando a Mahmoud Ahmadinejad con Hitler.

En América Latina, los cables también tuvieron un fuerte eco: en Argentina, se revelaron contactos entre el fiscal Alberto Nisman y la embajada estadounidense por la causa AMIA; en Colombia, se expusieron ejecuciones extrajudiciales cometidas por militares; y en Perú, la relación entre las fuerzas armadas y bandas de narcotraficantes en la selva.

El Cablegate marcó un antes y un después en la diplomacia internacional. Por un lado, mostró hasta qué punto la diplomacia y el espionaje suelen ir de la mano; por el otro, abrió la puerta a una era de mayor transparencia, aunque con enormes riesgos para la privacidad y la seguridad. Como señaló Kristinn Hrafnsson, editor jefe de WikiLeaks, los documentos permitieron reflexionar de manera más realista sobre las relaciones de poder en el mundo, aunque la verdad, muchas veces, resulte incómoda.

Las consecuencias no tardaron en llegar: Chelsea Manning fue condenada a 35 años de prisión en 2013, aunque su pena fue conmutada por Obama en 2017. En cambio, Julian Assange quedó perseguido judicialmente bajo la Ley de Espionaje de Estados Unidos y hasta hoy enfrenta un largo proceso legal, con debates internacionales sobre su extradición y sobre el alcance de la libertad de prensa.

El Cablegate no solo expuso secretos incómodos de la diplomacia estadounidense, sino que también dejó en evidencia la tensión permanente entre el derecho a la información, la seguridad de los Estados y el poder de la verdad en la era digital.

● 2011 – Archivos de Guantánamo

En 2011, WikiLeaks filtró más de 765 documentos secretos del ejército de Estados Unidos conocidos como los Archivos de Guantánamo. Estos informes revelaban información sobre los 779 prisioneros que pasaron por la cárcel ubicada en la Bahía de Guantánamo, en Cuba, desde su apertura en 2002. Los documentos, llamados Informes de Evaluación de Detenidos, eran elaborados por oficiales de la Fuerza de Tarea Conjunta de Guantánamo y enviados al Comando Sur de Estados Unidos. En ellos se incluían perfiles personales de cada detenido, evaluaciones médicas y psicológicas, supuestos vínculos con grupos terroristas y recomendaciones sobre sí mantenerlos presos, trasladarlos o liberarlos.

Las filtraciones mostraron que sólo una minoría de los prisioneros era considerada realmente peligrosa o vinculada a Al Qaeda, mientras que la mayoría eran combatientes de bajo rango o incluso personas inocentes capturadas por error. Muchas de las acusaciones se basaban en testimonios obtenidos bajo tortura, amenazas o sobornos, lo que hacía que la información fuera poco confiable. También se evidenció que varios detenidos fueron arrestados en Afganistán y Pakistán por tropas aliadas y entregados a Estados Unidos a cambio de recompensas económicas, sin pruebas sólidas en su contra.

Entre los casos más emblemáticos aparecen figuras como Abu Zubaydah, sometido al ahogamiento simulado más de 80 veces, y Mohammed al-Qahtani, acusado de ser el “20º secuestrador del 11-S”, quien fue víctima de torturas autorizadas directamente por el Pentágono. Además, se registraron siete muertes en custodia en circunstancias sospechosas, mientras que muchos otros prisioneros fueron liberados tras años de encierro sin que existieran cargos en su contra.

Los Archivos de Guantánamo dejaron en evidencia que la prisión no estaba llena de los “peores terroristas del mundo”, como sostenía el discurso oficial, sino que funcionó como un centro de detención arbitraria y de tortura sistemática. La mayoría de los prisioneros nunca tuvo vínculos comprobados con el terrorismo internacional, lo que convirtió a Guantánamo en un símbolo mundial de abuso de derechos humanos y en una de las filtraciones más significativas de WikiLeaks.

● 2017 - Vault 7

En marzo de 2017, WikiLeaks comenzó a publicar una serie de documentos clasificados bajo el nombre en clave **Vault 7**, que revelaban herramientas de espionaje digital desarrolladas por la CIA. El lanzamiento principal, llamado **“Year Zero”**, consistió en más de 8.700 documentos provenientes de una red de alta seguridad dentro del Centro de Ciberinteligencia de la CIA en Langley, Virginia.

Estos materiales expusieron que la CIA perdió el control del grueso de su arsenal digital, incluyendo malware, virus, troyanos, herramientas de control remoto y cientos de programas tipo “zero-day” (vulnerabilidades hasta ese momento desconocidas), sumando cientos de

millones de líneas de código y abarcando sistemas operativos y dispositivos populares. Los documentos muestran que la agencia desarrolló capacidades de espionaje capaces de comprometer smartphones (iOS y Android), navegadores web, sistemas operativos como Windows, macOS o Linux y hasta televisores inteligentes, como Samsung TVs, que podían ser convertidos en micrófonos encubiertos.

La CIA disponía de una división de hackers cada vez más poderosa y separada de la NSA, que para finales de 2016 contaba con más de 5.000 usuarios registrados y había desarrollado más de mil herramientas digitales ofensivas.

El contenido filtrado también incluye detalles técnicos de herramientas específicas como ‘Weeping Angel’ (convierte televisores en espías en modo "falso apagado"), ‘Grasshopper’ (malware modular para Windows) o el ‘Marble Framework’ (para ocultar el origen de malware)—proyectos que fueron publicados en distintas entregas posteriores

El origen de la filtración se atribuye a ex-hackers gubernamentales o contratistas, que distribuyeron estos archivos de forma no autorizada, uno de ellos entregó los materiales a WikiLeaks con el argumento de que el público debería debatir la seguridad, control y regulación de estas "ciberarmas"

La CIA respondió calificando a WikiLeaks como un "servicio de inteligencia hostil no estatal". Además, medios de prensa como Wired y Rolling Stone confirmaron la autenticidad de los documentos y destacaron su impacto al revelar el alarmante alcance del espionaje digital clandestino estadounidense

Los archivos **Vault 7** representan la mayor fuga de herramientas digitales de la CIA conocida hasta la fecha, exponiendo la magnitud de su arsenal cibernético y planteando serias preguntas sobre la supervisión pública, la ética en inteligencia y la seguridad global en la era digital.

Reacciones internacionales y consecuencias legales

En 2010, Wikileaks publicó un informe militar estadounidense de 2008 que afirmaba que las filtraciones de Wikileaks "podrían resultar en mayores amenazas para el personal, el equipo, las instalaciones o las instalaciones del Departamento de Defensa" El informe sugería un plan para identificar y exponer las fuentes de Wikileaks para "disuadir a otros de usar Wikileaks" y "destruir el centro de gravedad" de Wikileaks al atacar su fiabilidad.

En 2010, Bank of America contrató los servicios de un grupo de empresas de seguridad informática , conocidas como Team Themis. **En 2011**, el grupo hacktivista Anonymous publicó correos electrónicos de HBGary Federal que mostraban que Team Themis había propuesto un plan que sugería "difundir desinformación" e "interrumpir" el apoyo de Glenn Greenwald a WikiLeaks.] Team Themis planeaba exponer las operaciones de WikiLeaks mediante desinformación y ciberataques.

En diciembre de 2010, PayPal suspendió la cuenta de WikiLeaks después de recibir una carta del Departamento de Estado de los EE. UU. que caracterizaba las actividades de WikiLeaks como ilegales en los EE. UU. Mastercard y Visa Europe también dejaron de aceptar pagos a WikiLeaks después de la presión de los EE. UU.

En 2010, John Young, exmiembro del consejo asesor , acusó a la organización de falta de transparencia en su recaudación de fondos y gestión financiera. Afirmó su convicción de que WikiLeaks no podía garantizar a los denunciantes el anonimato ni la confidencialidad que afirmaba ofrecer

Tras la publicación por parte de WikiLeaks de documentos clasificados del gobierno estadounidense filtrados por Chelsea Manning , el entonces vicepresidente estadounidense Joe Biden declaró que "se acerca más a un terrorista de alta tecnología que a los Papeles del Pentágono ".

Biden afirmó que Assange "ha hecho cosas que han dañado y puesto en peligro las vidas y ocupaciones de personas en otras partes del mundo".

El representante Pete Hoekstra exigió medidas decisivas contra WikiLeaks.

Los senadores Joseph Lieberman y John McCain calificaron las publicaciones de WikiLeaks como la "vulneración de seguridad más perjudicial en la historia de este país" y el representante Peter T. King afirmó que WikiLeaks debería ser designada organización terrorista .

Sarah Palin , William Kristol y Rick Santorum compraron a WikiLeaks con un grupo terrorista.

El senador John Ensign propuso modificar la Ley de Espionaje para atacar a WikiLeaks.

En 2015, el representante Mac Thornberry afirmó que las publicaciones de WikiLeaks habían causado un daño enorme y ayudado a los principales adversarios del país.

Tras calificar a WikiLeaks de "vergonzoso" en 2010, el presidente electo Donald Trump elogió a WikiLeaks en octubre de 2016, diciendo: "Me encanta WikiLeaks"

Newt Gingrich , quien pidió que Assange fuera "tratado como un combatiente enemigo" en 2010, lo elogió como un "entrevistado realista y directo"

- Empresas que retiraron apoyo.

El 22 de enero de 2010, PayPal, el intermediario de pagos por internet, suspendió la cuenta de WikiLeaks y congeló sus activos. WikiLeaks afirmó que esto ya había ocurrido antes y que se hizo sin motivo aparente.

En agosto de 2010, Moneybookers , la empresa de pagos por internet, cerró la cuenta de WikiLeaks y envió cartas a Assange indicando que el cierre de la cuenta se produjo tras una auditoría "para cumplir con investigaciones de blanqueo de capitales u otras investigaciones realizadas por las autoridades gubernamentales".

En diciembre de 2010, PayPal suspendió la cuenta de WikiLeaks. PayPal dijo que había tomado medidas después de que el Departamento de Estado de EE. UU. enviará una carta a Wikileaks declarando que las actividades de Wikileaks eran ilegales en EE. UU

Mastercard , Visa Europe , Bank of America , Amazon , Western Union y el banco suizo PostFinance dejaron de tratar con WikiLeaks.

La única empresa que pareció apoyar a Wikileak fue Datacell ya que fue la única empresa que aceptar donaciones con tarjetas de crédito y débito y amenazó a Mastercard y Visa con acciones legales para hacer cumplir la reanudación de los pagos a WikiLeaks ya que dice que sus acciones fue el resultado de la presión política.

Tras un ataque de denegación de servicio , WikiLeaks trasladó su sitio web a los servidores de Amazon . Posteriormente, Amazon eliminó el sitio web, En una declaración pública, Amazon afirmó que WikiLeaks no estaba cumpliendo con sus términos de servicio.

A raíz de esto **En octubre de 2011,** Assange dijo que el bloqueo financiero le había costado a WikiLeaks el noventa y cinco por ciento de sus ingresos

- Procesos judiciales contra Julian Assange.

En 1987, Assange fue sospechoso de participar en un hackeo a Citibank que supuestamente involucra el robo de $500,000. La policía allanó la casa de su madre y confiscó su equipo. No se presentaron cargos y el equipo fue devuelto.

En 1991 Assange y el grupo International Subversives supuestamente accedieron a MILNET, una red de datos del ejército estadounidense. Assange afirmó que tuvieron "control durante dos años". **En 2012**, un oficial de la Policía Federal Australiana declaró que no había evidencia de este hackeo, pero que si se encontrara pruebas de que Assange está relacionado aun podría ser enjuiciado.

En 1991 Assange fue detenido por la Policía Federal Australiana acusado de acceder de modo ilegal a varias computadoras. **En 1994** fue acusado de 31 cargos por delitos informáticos. **En 1996** se declaró culpable de 25 cargos por delitos informáticos y fue multado por AU$2500 y puesto en libertad con una fianza de AU$5000 por buena conducta.

En 2010 La fiscalía sueca emitió una orden de arresto contra Assange por presunta violación, coacción ilícita y abuso sexual. Assange negó los cargos y dijo que eran una excusa política. **En 2012,** huyó a la embajada de Ecuador en Londres. **En 2019,** Suecia cerró el caso por el pasar del tiempo las pruebas perdieron fuerzas a pesar de venir que gente de confianza.

En 2010 EE. UU. inició una investigación penal. **En 2019,** la fiscalía estadounidense lo acusó bajo la Ley de Espionaje y fue acusado de 18 cargos por espionaje y 1 cargo por conspiración informática.

En 2012 para evitar la extradición a Suecia y EE. UU., Assange solicitó asilo diplomático. Ecuador se lo concedió hasta 2019, Tras perder el asilo, fue arrestado por la policía británica y condenado a 50 semanas de prisión por violar la libertad condicional al no presentarse en 2012

En 2019 EE. UU. solicitó su extradición para juzgarlo por espionaje. **En junio de 2024**, llegó a un acuerdo con el Departamento de Justicia de EE. UU. y se declaró culpable de un cargo menor y quedó en libertad.h

Wikileaks y la libertad de información

- Relación con el periodismo de investigación.

WikiLeaks ha marcado un antes y un después en la historia del periodismo de investigación. Desde su fundación en 2006 por Julian Assange, la plataforma se convirtió en un espacio destinado a la filtración de documentos confidenciales de interés público, permitiendo que periodistas de todo el mundo pudieran acceder a información que, de otro modo, habría permanecido oculta.

El español Pepe Rodríguez, especialista en periodismo investigativo —autor y docente universitario— enumera aspectos que confluyen en quienes practican el periodismo investigativo. El periodista investigador, *"utiliza técnicas habituales de la profesión u otras específicas y/o habitualmente atribuibles a profesiones ajenas a la suya (detective, policía, abogado, historiador, etc.) elabora una información producto de un número indeterminado de fuentes (atribuibles o no) y de un análisis personal de datos, contrastados con mayor o menor eficacia, le conducen a comunicar una noticia sobre una realidad, que por su configuración y naturaleza, estaba destinada a permanecer oculta durante un período de tiempo indefinido (…)"*. Añade un elemento crucial. Sin la revelación de dicha información, *"nunca o muy difícilmente hubiese podido aflorar"*. Las filtraciones de Wikileaks reúnen todas estas características. No hay por donde equivocarse. Assange es periodista.

Una de las principales aportaciones de WikiLeaks al periodismo de investigación ha sido su modelo de colaboración con medios internacionales. Casos emblemáticos como la publicación de los *Diarios de Guerra de Afganistán* y los *Papeles de Irak* en 2010 fueron posibles gracias a alianzas con periódicos de gran prestigio, como *The Guardian*, *The New York Times*, *Der Spiegel*, *Le Monde* y *El País*. Estas colaboraciones demostraron que la filtración de información masiva podía complementarse con la investigación periodística tradicional, donde los medios analizaron, contextualizan y verifican los datos para hacerlos comprensibles al público.

Además, WikiLeaks impulsó el debate sobre **l**os límites entre activismo digital y periodismo profesional. Mientras algunos críticos señalaron que la organización actuaba como una "plataforma de publicación" más que como un medio periodístico en sí mismo, otros destacaron que sin su labor de obtención y resguardo de documentos, los periodistas no habrían podido desarrollar investigaciones de gran impacto mundial.

El aporte de WikiLeaks también evidenció la importancia del cifrado y el anonimato en la labor periodística. Muchos periodistas de investigación, especialmente aquellos que trabajan con fuentes en contextos de riesgo, comenzaron a adoptar herramientas de seguridad digital inspiradas en las prácticas de WikiLeaks, lo que transformó las rutinas profesionales y elevó los estándares de protección de la información y las fuentes.

WikiLeaks no solo funcionó como un canal para la transparencia, sino que también redefinió la relación entre las filtraciones, las fuentes y los periodistas, consolidando la idea de que la cooperación entre plataformas digitales y medios tradicionales puede potenciar el alcance del periodismo de investigación y contribuir al derecho ciudadano a la información.

- Uso de herramientas de cifrado y anonimato.

Una de las cosas más importantes de este medio es mantener el anonimato de los informantes y para lograr dicha «ocultación» se valen de software de código abierto, que es lo que nos convoca en esta ocasión.

La misión consiste básicamente, en que la persona que colabore con el medio, no pueda ser detectada. Como sabemos hay múltiples maneras de rastrear a una persona, desde un simple y automático ping, hasta triangulación por wifi, por lo que la tarea no es tan simple, menos en este caso, donde no hay que dejar ningún tipo de rastro que dé indicio de quién, dónde y cómo se efectuó esa filtración de información ¿cómo lograrlo? bueno, haciendo uso y combinación de múltiples herramientas de Software Libre.

OpenSSL

Es un conjunto de herramientas que implementa protocolos criptográficos como SSL (Secure Sockets Layer) y TLS (Transport Layer Security). Su función principal es proteger la confidencialidad e integridad de las comunicaciones en Internet, mediante el cifrado de datos y autenticación de servidores y clientes. Es ampliamente utilizada en navegadores, servidores web y aplicaciones que requieren seguridad en la transmisión de información sensible, como contraseñas o datos bancarios.

Lógicamente Wikileaks utiliza esta herramienta para mantener accesos seguros a sus servidores y ayudar en el cifrado de información, pero esta medida, que ya es prácticamente un estándar, es sólo una de las herramientas que se necesitan para mantener la seguridad.

Freenet

Es una red diseñada especialmente para combatir la posible censura de información a la vez que mantener el anonimato de sus usuarios mientras navegan, comparten y publican información en ella, tiene un funcionamiento similar a las redes P2P de manera que los nodos pueden intercambiar información entre ellos de forma descentralizada y anónima, ya que la comunicación entre nodos se cifra.

Funciona mediante un sistema distribuido de almacenamiento, en el cual los usuarios aportan parte de sus recursos de red y disco duro para alojar fragmentos de datos cifrados. De esta manera, ningún nodo tiene control total sobre la información, lo que dificulta la censura y el rastreo de los contenidos. Según EcuRed y estudios sobre redes anónimas,

Freenet se ha utilizado como espacio de libertad de expresión en contextos de censura estatal, aunque también ha sido criticada por permitir la difusión de contenidos ilegales.

Además usando Freenet se puede crear una «red oscura», la cual pueden crear y mantener entre algunos amigos para intercambiar información y que se vuelve muy difícil de detectar

Tor (The Onion Router)

Es una red de anonimato que enruta el tráfico de los usuarios a través de múltiples nodos voluntarios en todo el mundo, aplicando un sistema de cifrado en capas —similar a una cebolla—. Este proceso oculta la dirección IP de origen y destino, haciendo muy difícil rastrear la actividad en línea. Tor se utiliza tanto para proteger la privacidad de usuarios comunes y periodistas en regímenes autoritarios, como para acceder a la llamada “Deep Web” o “Dark Web”. Fuentes como *El País* destacan que, aunque Tor es una herramienta esencial para la libertad de información, también ha sido asociada con mercados ilegales y actividades delictivas, lo que genera un debate sobre su regulación.

Hay que destacar que Tor no solo le puede dar anonimato a un usuario, sino también a un servidor anfitrión (y a varios de ellos), lo que lo convierte **e**n una de las mayores armas de anonimato para Wikileaks en la red.

PGP (Pretty Good Privacy)

Es un sistema de cifrado desarrollado por Phil Zimmermann en 1991, diseñado para proteger la comunicación electrónica. Utiliza una combinación de cifrado simétrico y asimétrico, junto con firmas digitales, lo que permite garantizar la confidencialidad, autenticidad e integridad de los mensajes. PGP se popularizó en el intercambio de correos electrónicos seguros y en la verificación de archivos descargados de Internet. De acuerdo con la documentación técnica, su importancia radica en ofrecer a los usuarios una herramienta robusta de seguridad sin depender de corporaciones o gobiernos, lo que lo convirtió en un símbolo del movimiento “cypherpunk” y de la defensa de la privacidad digital.

PGP proporciona uno de los mejores servicios de cifrado e igualmente se hace evidente la razón de su uso por parte de Wikileaks, este sistema destinado a proteger la privacidad es otra de las armas de este servicio de contenidos e información más controvertido de los últimos tiempos.

Por último, solo destacar que Wikileaks hace uso de Mediawiki**,** el software de código abierto licenciado bajo la GNU que se utiliza en Wikipedia y en muchas otras wikis, el cual está especialmente diseñado y preparado para la generación de contenidos.

- Debate: libertad de prensa vs. seguridad nacional.

La libertad de expresión es un derecho humano reconocido internacionalmente que limita la capacidad del Estado para prohibir recibir y publicar información. Corresponde al Estado demostrar que cualquier restricción que imponga es necesaria, proporcionada y compatible con el derecho a la libertad de expresión.

Según Amnistía Internacional, los procedimientos penales destinados a castigar a una persona por comunicar indicios de violaciones de derechos humanos nunca están justificados. Lo mismo aplica para la publicación de información sobre otras cuestiones de interés público. Gran parte de los documentos publicados por WikiLeaks parecen pertenecer a estas categorías, por lo que cualquier enjuiciamiento basado en ellos sería incompatible con la libertad de expresión. Amnistía Internacional también señala que, hasta la fecha, no hay acusaciones formales contra Julian Assange por la publicación de estos documentos, por lo que no es posible opinar sobre un posible proceso judicial en su contra.

El caso de WikiLeaks ha generado un debate central sobre la tensión entre la libertad de prensa y la seguridad nacional. La filtración de miles de documentos clasificados, como los cables diplomáticos de Estados Unidos en 2010, abrió la discusión sobre los límites de la transparencia y el derecho a la información frente a los riesgos que podrían derivarse para la seguridad de los Estados.

Por un lado, la libertad de prensa es esencial en las sociedades democráticas, ya que permite a la ciudadanía ejercer control sobre el poder político y militar. Organizaciones como Reporteros Sin Fronteras y medios como *El País* y *El Mundo* consideran que WikiLeaks representó una forma de “periodismo radical de datos”, orientado a exponer violaciones de derechos humanos, corrupción y abusos de poder que de otro modo permanecerán ocultos. Desde esta perspectiva, la publicación de documentos clasificados es legítima cuando contribuye al interés público y fortalece la rendición de cuentas.

Por otro lado, los gobiernos, especialmente Estados Unidos, han argumentado que la difusión de información sensible puede comprometer la seguridad nacional, afectando operaciones militares, diplomáticas y la vida de agentes en el terreno. Este tipo de filtraciones masivas genera un dilema: aunque fortalecen la transparencia, también pueden afectar la estabilidad política y diplomática.

El caso de WikiLeaks evidencia la tensión estructural entre el derecho a informar y el deber de proteger la seguridad del Estado. Mientras que el periodismo de investigación tradicional selecciona y contextualiza cuidadosamente los documentos antes de publicarlos, WikiLeaks optó por un modelo de máxima transparencia, lo que llevó a cuestionar cómo equilibrar la libertad de expresión con la responsabilidad de no causar daños colaterales.

Detalles tecnicos

- Seguridad y anonimato

Todo el personal que trabaja con fuentes está acreditado como periodista. Todas las presentaciones establecen una relación periodista-fuente. Las presentaciones en línea se canalizan a través de Suecia y Bélgica, países con leyes de protección de fuentes y periodistas de primera categoría. En Suecia, la ley no solo protege contra cualquier investigación oficial sobre las fuentes de los periodistas, sino que también permite que una fuente cuya identidad haya sido revelada sin autorización inicie acciones penales contra un periodista infiel que haya incumplido su promesa de confidencialidad.

WikiLeaks no registra ninguna información que identifique a las fuentes y existen numerosos mecanismos de envío disponibles para manejar incluso la información de seguridad nacional más sensible.

WikiLeaks es el ganador del premio a la Libertad de Expresión del Índice Economist sobre Censura de 2008 y del premio de información sobre derechos humanos de 2009 de Amnistía Internacional (Nuevos Medios).

WikiLeaks tiene un historial de revelar noticias importantes en todos los principales medios de comunicación y de proteger con firmeza las fuentes y la libertad de prensa. **Ninguna fuente ha sido expuesta jamás ni ningún material ha sido censurado** . Desde su creación a principios de 2007, WikiLeaks ha triunfado ante todos los ataques legales (e ilegales), incluyendo los del Pentágono, la Oficina de Seguridad Pública de China, el expresidente de Kenia, el primer ministro de Bermudas, la Cienciología, la Iglesia Católica y la Iglesia Mormona, el mayor banco privado suizo y empresas rusas. WikiLeaks ha publicado más documentos de inteligencia clasificados que el resto de la prensa mundial en conjunto.

Envíos mediante carga segura

Rápido, sencillo y automático con el mejor cifrado de nivel bancario. No guardamos registros de dónde subiste el archivo, tu zona horaria, navegador ni siquiera de cuándo lo enviaste (si eliges un *retraso de publicación* distinto de cero , configuramos el registro de tiempo del archivo con la fecha de publicación más una hora aleatoria dentro de ese día).

Si envía anónimamente un **archivo de Microsoft Word (.doc") que haya editado en algún momento** , intente enviar un documento PDF (.pdf"), ya que los documentos de Word

pueden incluir su nombre o el nombre de su computadora. Consulte **la sección de redacción de archivos de Word** para obtener más información. Si no tiene los medios para generar un archivo PDF, el personal de WikiLeaks lo convertirá.

También puede utilizar la red segura TOR

(red segura, anónima y distribuida para máxima seguridad).

Envíos a través de nuestra discreta red postal

Los envíos a nuestra red postal ofrecen la **forma más fuerte de anonimato** y son buenos para decir la verdad en masa.

Pasos:

1. Primero, guarde la fuga en un disquete, CD, DVD o memoria USB . Si usa disquetes, cree dos, ya que suelen ser poco fiables. Si solo tiene documentos en papel, los escaneamos si son de gran interés político o mediático
2. Envíe su información a uno de nuestros facilitadores de confianza que figuran a continuación. Puede enviarla al país que considere más adecuado según la naturaleza del material y su servicio postal. Si el sistema postal de su país no es confiable, puede enviar varias copias, utilizar DHL, FedEx u otro servicio de mensajería.

Los facilitadores de WikiLeaks subirán su envío usando su conexión rápida a internet. Si usa un disquete, asegúrese de enviar dos para mayor fiabilidad.

Puede utilizar cualquier dirección de devolución que desee, pero asegúrese doblemente de haber escrito correctamente el destino, ya que los trabajadores postales no podrán devolverle el sobre.

Después de recibir su envío postal, nuestros facilitadores cargan los datos en WikiLeaks y luego destruyen el paquete enviado.

Envíos postales de alto riesgo

Si la fuga supone un riesgo extremadamente alto, es posible que desee enviar el correo lejos de su oficina de correos local, a un lugar que no tenga testigos ni vigilancia por video.

Muchas grabadoras de CD y DVD incluyen el número de serie de la grabadora de DVD o CD en los CD/DVD que graba. Si se intercepta el correo, esta información podría utilizarse, en teoría, para localizar al fabricante y, con su cooperación, al distribuidor, al agente de

ventas, etc. Considere si existen registros financieros que lo vinculen con la venta de la grabadora de CD/DVD si su adversario es capaz de interceptar la carta que nos envía y está dispuesto a realizar este tipo de costosa investigación.

De manera similar, los propios soportes de CD y DVD incluyen un "número de lote" de fabricación no único para cada grupo de alrededor de 10.000 CD/DVD fabricados.

Aunque no tenemos conocimiento de **ningún caso** en que lo anterior se haya utilizado con éxito para rastrear a un individuo, las operaciones antipiratería han utilizado la información para rastrear a organizaciones de piratería que venden decenas o cientos de miles de CD o DVD falsificados.

Si sospecha que está bajo vigilancia física, entregue la carta a un amigo o familiar de confianza para que la envíe por correo. En raras ocasiones, se ha seguido a personas que han sido objeto de vigilancia política importante hasta la oficina de correos y se les ha confiscado el correo de forma encubierta. En este caso excepcional, si no tiene intención de cifrar los datos y si la policía o los servicios de inteligencia de su país cuentan con los recursos necesarios para realizar análisis de ADN o huellas dactilares, le recomendamos tomar las precauciones adecuadas.

Wikileaks: Tor

El siguiente método requiere cierta habilidad técnica. Si está acostumbrado a instalar software nuevo y configurar servidores proxy, debería tener las habilidades necesarias; de lo contrario, puede utilizar uno de nuestros otros métodos de envío.

Tor, o The Onion Router, es una técnica criptográfica implementada inicialmente por investigadores de la Marina de los EE. UU. para permitir a los agentes de inteligencia usar internet sin ser rastreados, cifrando y enrutando las comunicaciones a través de numerosos servidores. Posteriormente, Tor fue desarrollado por la universidad estadounidense MIT y por la Electronic Frontier Foundation , organismo de control de los derechos en internet de California , y posteriormente incorporado a Wikileaks .

Usando nuestro paquete de acceso anónimo puedes evitar que los espías de Internet sepan que tu ordenador se ha conectado a Wikileaks .

La mayoría de los Wikileaks no necesitan esta seguridad adicional, y existen alternativas más sencillas y posiblemente más seguras para filtraciones puntuales de alto riesgo. Pero para quienes corren riesgo y desean acceder a Wikileaks desde la comodidad de sus

hogares u oficinas, o necesitan eludir la censura de internet, Tor (enrutamiento cebolla) es una excelente solución.

Una vez instalado nuestro paquete de acceso a Tor (ver más abajo), podrá conectarse a Wikileaks a través de nuestra dirección anónima («.onion» significa «Onion Routing», pero no necesita preocuparse por este detalle). *Nota: el enlace* .onion original para navegar *por Wikileaks no está disponible actualmente; sin embargo, si ha instalado Tor y redirige toda su navegación a través de la red Tor, podrá navegar por el sitio web normal de Wikileaks con un alto grado de anonimato (pero sin cifrado de extremo a extremo). La dirección* .onion segura *proporcionada aquí y en la página de envíos debería funcionar en cualquier caso.* Para cargar un documento de forma anónima usando Tor:

> http://suw74isz7wqzpmgu.onion/
> (**este enlace solo funcionará una vez que haya instalado y configurado Tor**).

A menos que tenga una memoria excelente, quizá desee anotar esa dirección (o tal vez destruir el papel cuando haya terminado de usarlo).

Sin Tor, al acceder a un sitio de Wikileaks de la forma habitual, por ejemplo, a través de https://wikileaks.org/, todos tus datos están cifrados, pero los espías de internet podrían registrar cuánto tiempo pasó tu ordenador comunicándose con los servidores de Wikileaks.

Wikileaks Tor utiliza **conexiones anónimas de extremo a extremo totalmente cifradas** . Es imposible una configuración incorrecta accidental y en ningún momento tu comunicación sale de la red cifrada.

El costo de este anonimato es la velocidad: las páginas tardan en promedio 15 segundos en cargarse, pero a veces hasta 60. Las cargas de archivos a nuestros servidores tienden a ocurrir a una velocidad de 5 a 30 kilobytes por segundo.

● Resiliencia y prevención de censura

Servidores espejo

Un servidor es un computador que está diseñado para proporcionar servicios a otros dispositivos conectados a la red. Estos servicios incluyen almacenamiento de archivos, accesos remotos, acceso a bases de datos y servicios web.
El término "espejo" se refiere a la duplicación de los datos en dos o más servidores o dispositivos de almacenamiento

Los servidores espejos son servidores que replican exactamente al servidor principal se utilizan para garantizar disponibilidad de servicios. Se utilizan para prevenir la saturación de una red, por lo tanto estar siempre disponible.
Los servidores espejo tienen diferentes usos, pero principalmente se utilizan para mejorar la velocidad de descarga y reducir la carga del servidor original.
Cuando alguien descarga archivos de un sitio web, puede crear un cuello de botella en el servidor, lo que resulta en una experiencia de usuario lenta e insatisfactoria. Al tener un servidor espejo, los usuarios pueden descargar archivos de la copia más cercana a ellos, lo que reduce la cantidad de tráfico en el servidor principal y acelera la descarga.
Otro uso importante de los servidores espejo es para la recuperación de desastres. Si el servidor primario falla o se pierde, la copia de seguridad en el servidor espejo puede hacerse cargo rápidamente y continuar sirviendo a los usuarios sin interrupciones. Esto garantiza la continuidad del negocio y la satisfacción del cliente.
Los servidores espejo funcionan como copias exactas y actualizadas del servidor principal, replicando todo su contenido, incluyendo el sistema operativo, servicios, aplicaciones, configuraciones y bases de datos, para garantizar que ambos sistemas sean idénticos en todo momento.

Además pueden estar situados en distintos lugares para poder garantizar el acceso a la mayor cantidad de personas en caso de tener alcance global, también mejora la velocidad y confiabilidad frente a diferentes problemas que pueda tener alguno de estos.

wikileaks utiliza los servidores espejo para:
evitar la censura debido a las veces su dominio fue dado de baja por múltiples proveedores permite el acceso continuo a los datos incluso si el dispositivo de origen deja de estar disponible, la copia reflejada puede tomar el control sin problemas. Por ejemplo cuando Amazon los expulsó de sus servidores aduciendo que la organización violaba sus términos y condiciones de servicio. (BBC News, 8 diciembre 2010)

resistir ataques: wikileaks fue objeto de múltiples ciberataques esto ayuda minimizando el tiempo de inactividad y garantizando operaciones ininterrumpidas
descentralizar el acceso: los usuarios tienen múltiples puntos donde acceder a la información.
Los servidores espejo son el escudo digital de WikiLeaks: una forma de asegurar que la información filtrada permanezca disponible.

- **Protección contra ataques DDoS**.

Un ataque de denegación de servicio distribuido (DDoS) es un intento malintencionado de interrumpir el tráfico normal de un servidor, servicio o red determinada, sobrecargando el objetivo o su infraestructura asociada con una avalancha de tráfico de Internet.

La efectividad de los ataques DDoS reside en el uso de sistemas informáticos vulnerables desde los que se origina el ataque de tráfico. Entre los equipos afectados puede haber ordenadores y otros recursos de red, tales como dispositivos IoT.

Cómo funcionan los ataques DDoS

Los ataques DDoS se llevan a cabo con redes de equipos conectados a Internet.
Estas redes constan de ordenadores y otros dispositivos que han sido infectados con malware, lo que permite a un atacante controlarlos de forma remota. Estos dispositivos individuales se denominan bots (o zombies), y un grupo de bots recibe el nombre de botnet.

Cuando el servidor o la red de una víctima es el blanco de una botnet, cada bot envía solicitudes a la dirección IP del destino, lo que puede llegar a sobrecargar el servidor o la red y, por consiguiente, provocar una denegación de servicio al tráfico normal.(Cloudflare, s.f.)

Un ataque DDoS bien coordinado suele desplegarse en varias fases:

- Reconocimiento: El atacante identifica los servicios expuestos, su arquitectura y posibles puntos débiles, como servidores con protección limitada o configuraciones por defecto.
- Compromiso de dispositivos: Se infectan múltiples equipos para formar la botnet. Estos pueden incluir desde ordenadores personales hasta dispositivos IoT mal asegurados.
- Comando y control (C2): Se establece un canal de comunicación entre los dispositivos comprometidos y el servidor de control, desde el cual se orquestará el ataque.
- Ejecución: Se lanza la ofensiva en el momento más crítico, en muchas ocasiones coincidiendo con eventos clave o durante campañas específicas, con el objetivo de maximizar el impacto.
- Adaptación: Algunos ataques monitorizan en tiempo real las respuestas defensivas de la víctima y ajustan su patrón de tráfico para evadir las medidas de mitigación.

WikiLeaks comenzó a sufrir ataques DDoS cuando anunció que publicaría cables diplomáticos de EE.UU. Posteriormente su proveedor de dominio (la dirección que se usa en internet) suspendió su cuenta alegando que recibía demasiados ataques lo que ponía en riesgo su servicio a otros clientes.
Wikileaks sufrió estos ataques que buscaban inutilizar su sitio web para impedir el acceso a documentos filtrados que comprometían a gobiernos y corporaciones.

Para contrarrestar los ataques, WikiLeaks pidió ayuda a sus seguidores, quienes crearon cientos de servidores espejo que replicaban el contenido original.
A su vez el colectivo Anonymous lanzó ataques DDoS contra entidades que bloquearon donaciones a WikiLeaks, como Visa, Mastercard y PayPal.

La preocupación principal a la hora de mitigar un ataque DDoS es diferenciar entre el ataque de tráfico y el tráfico normal.
Por lo general, cuanto más complejo sea el ataque, más difícil será distinguir el tráfico normal del malintencionado. El objetivo del atacante es disimularlo en la medida de lo posible y hacer que la mitigación sea lo más ineficaz posible.

- **Limitación de velocidad**

La limitación de velocidad puede ser un método eficaz para prevenir ataques DDoS . Funciona limitando la cantidad de solicitudes que un usuario (o bot) puede realizar a un servicio o servidor en un período determinado. La limitación de velocidad logra su objetivo impidiendo que ciertos usuarios, o grupos de usuarios, monopolicen el acceso al activo y lo dejen indisponible.

Hay tres tipos clave de limitación de velocidad, que se describen a continuación:

Limitación de velocidad basada en el usuario : Restringe el acceso según el usuario específico que realiza la solicitud, basándose en su dirección IP u otros identificadores. Esto ayuda a prevenir ataques de credenciales, además de ataques DDoS.
Limitación de velocidad geográfica : Limita la cantidad de solicitudes que pueden provenir de una ubicación o región determinada.
Limitación de velocidad basada en el tiempo : Este método utiliza marcas de tiempo de las solicitudes para limitar su frecuencia.(Netscout, 10 Marzo 2024)

- **Firewalls**

Un firewall de red es un sistema de seguridad que supervisa y controla el tráfico de red, tanto entrante como saliente, para proteger una red privada de accesos no autorizados y amenazas cibernéticas.

El caso de uso primario de un firewall es la seguridad. Los firewalls pueden interceptar el tráfico malicioso entrante antes de que alcance la red, así como impedir que la información confidencial salga de la misma.

Firewalls de aplicaciones web(WAF)

Los WAF ayudan a proteger las aplicaciones web de los usuarios con intenciones maliciosas. Un WAF ayuda a proteger las aplicaciones web filtrando y supervisando el tráfico HTTP entre una aplicación web e Internet. Suele proteger las aplicaciones web de

ataques como falsificación entre sitios, scripting entre sitios (XSS), inclusión de archivos e inyección de código SQL, entre otros.

El WAF opera por medio de un conjunto de reglas, normalmente denominadas directivas. Estas directivas tienen el fin de proteger contra vulnerabilidades en la aplicación mediante la filtración del tráfico malicioso. El valor de un WAF procede, en parte, de la velocidad y facilidad con que se pueden aplicar modificaciones en las directivas que permiten una respuesta más rápida ante diversos vectores de ataque; durante un ataque DDoS, se puede implementar rápidamente la limitación de velocidad modificando las directivas del WAF.

- **Cifrado de tráfico (HTTPS/SSL)** y direcciones dinámicas .onion en Tor.

El protocolo de transferencia de hipertexto seguro (HTTPS) es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web.
Cualquier sitio web, especialmente los que requieren credenciales de inicio de sesión, debe utilizar HTTPS
HTTPS utiliza un protocolo de encriptación para encriptar las comunicaciones. mediante Secure Sockets Layer (SSL).
Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Capa de sockets seguros y su sucesor TLS (Transport Layer Security): Son protocolos criptográficos que permiten el cifrado de la información en tránsito.

El certificado SSL mantiene seguras las conexiones a Internet y evita que los delincuentes lean o modifiquen la información transferida entre dos sistemas.
Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita que se pueda leer la información que se envía a través de la conexión antes de que llegue a destino.

El proceso funciona de la siguiente manera:

- Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL.
- El navegador o servidor solicita que el servidor web se identifique.
- En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL.
- El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web.
- el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL.
- Los datos cifrados se comparten entre el navegador o servidor y el servidor web.

Conclusión

La investigación sobre el caso Wikileaks 2006 demuestra cómo la tecnología puede convertirse en una herramienta poderosa para promover la transparencia y el acceso a la información. Gracias al uso de programación web, cifrado, anonimato y redes distribuidas, fue posible filtrar documentos confidenciales sin que la identidad de los informantes se viera comprometida, y al mismo tiempo evitar bloqueos o censuras impuestas por gobiernos o instituciones. Este caso evidencia que, con las herramientas técnicas adecuadas, la información puede circular de manera segura y masiva, permitiendo que la verdad llegue a la sociedad incluso frente a intentos de restricción. En definitiva, Wikileaks muestra que la tecnología no solo amplía nuestras capacidades de comunicación, sino que también puede fortalecer la transparencia y la rendición de cuentas en contextos donde otras vías serían limitadas.

Referencias

Amnistía Internacional. (16 diciembre 2010). *Preguntas y respuestas: Wikileaks y la libertad de expresión.* www.amnesty.org. https://www.amnesty.org/es/latest/news/2010/12/preguntas-respuestas-wikileaks-y-libertad-expresion/

BBC News.(8 diciembre 2010) *El "ejército" de WikiLeaks*. www.bbc.com https://www.bbc.com/mundo/noticias/2010/12/101208_1009_wikileaks_activistas_ataques_ddos_dc

Cloudflare. (s.f).*¿Qué es un ataque DoS?*. www.Cloudflare.com https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

Cloudflare. (s.f.).*¿Qué es un firewall? Cómo funcionan los firewalls de red*. www.Cloudflare.com. https://www.cloudflare.com/es-es/learning/security/what-is-a-firewall/

WikiLeaks. (2025, julio 11). Wikipedia, la Enciclopedia Libre. https://es.wikipedia.org/wiki/WikiLeaks

Khatchadourian, R. “No secrets”. (7 de junio de 2010). Wikileaks: breve historia. *Columbia University.* https://ccnmtl.columbia.edu/projects/caseconsortium/casestudies/109/casestudy/www/layout/case_id_109_id_743.html

Klimentov, M . (25 de junio de 2014). *Cronología: los momentos clave para WikiLeaks y Julian Assange*. www.infobae.com.ar: https://www.infobae.com/wapo/2024/06/25/cronologia-momentos-clave-para-wikileaks-y-julian-assange/?gad_source=1&gad_campaignid=20993778607&gclid=Cj0KCQjwqqDFBhDhARIsAIHTlktdA5hnerk29sp-n7y-uTpdG7IyzlJlSjRd6OZAV9tVieuWUlM0OfYaAjHyEALw_wcB

Netscout. (8 marzo 2024) *¿Qué es la limitación de velocidad para ataques DDoS?* netscout https://www-netscout-com.translate.goog/what-is/rate-limiting?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Nismrc.(26 de octubre de 2010). *Las tecnologías abiertas tras el anonimato de Wikileaks.* www.muylinux.com. https://www.muylinux.com/2010/10/26/las-tecnologias-abiertas-tras-el-anonimato-de-wikileaks/

Ray, M. (2025). WikiLeaks. www.britannica.com: https://www.britannica.com/topic/WikiLeaks

Redacción. (2011, 25 abril). WikiLeaks difunde documentos secretos sobre abusos en la cárcel de Guantánamo. *La Vanguardia*. https://www.lavanguardia.com/internacional/20110425/54144725745/wikileaks-difunde-documentos-secretos-sobre-abusos-en-la-carcel-de-guantanamo.html

Spiegel, D. (2010, 22 octubre).*Greatest Data Leak in US Military History*. Spiegel. https://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html

Vassallo, G. (2021, 28 noviembre). A once años del Cablegate, la explosiva filtración de cables diplomáticos de Estados Unidos. *PAGINA12*. https://www.pagina12.com.ar/385649-a-once-anos-del-cablegate-la-explosiva-filtracion-de-cables-

Villanueva, G. (23 de junio de 2019). *Assange, periodismo e infotecnologías.* Confidencial.digital.https://confidencial.digital/opinion/assange-periodismo-e-infotecnologias/?utm_source

Wikileaks. (s. f.).The WIKILEAKS Public Library of US Diplomacy. WikiLeaks https://search.wikileaks.org/plusd/about/

Wikileaks. (s. f.).Vault 7: *CIA Hacking Tools Revealed.* WikiLeaks https://wikileaks.org/ciav7p1/

WikiLeaks. (s. f.).*WikiLeaks:Submissions*. WikiLeaks https://wikileaks.org/wiki/WikiLeaks:Submissions

Wikileaks. (s. f.).*WikiLeaks Reveals Secret Files on All Guantánamo Prisoners* https://wikileaks.org/gitmo/

Wikileaks. (s.f.) *WikiLeaks:Tor*. WikiLeaks. https://wikileaks.org/wiki/WikiLeaks:Tor